Global Information Grid (GIG), Net Centricity (NC), Unique Identification (UID), Wide Area Workflow (WAWF) and Radio Frequency Identification (RFID) Initiatives

Overview and Impact on DPAS

Summary of topics

- Net centric information environment
- Global Information Grid (GIG)
- Net-Centric Reference Model
- Enterprise Information Environment (EIE)
- Net Centric data strategy and attributes
- UID
- WAWF
- RFID
- Impact to DPAS

The vision…

Net-centric Information Environment:

An information environment that utilizes emerging standards and technologies to optimize assured information sharing among all users. It results from implementing Global Information Grid (GIG) component architectures in accordance with the NCOW RM. A net-centric information environment is inclusive of Core and Community of Interest (COI) enterprise services, and a data sharing strategy that emphasizes metadata concepts and shared information spaces.

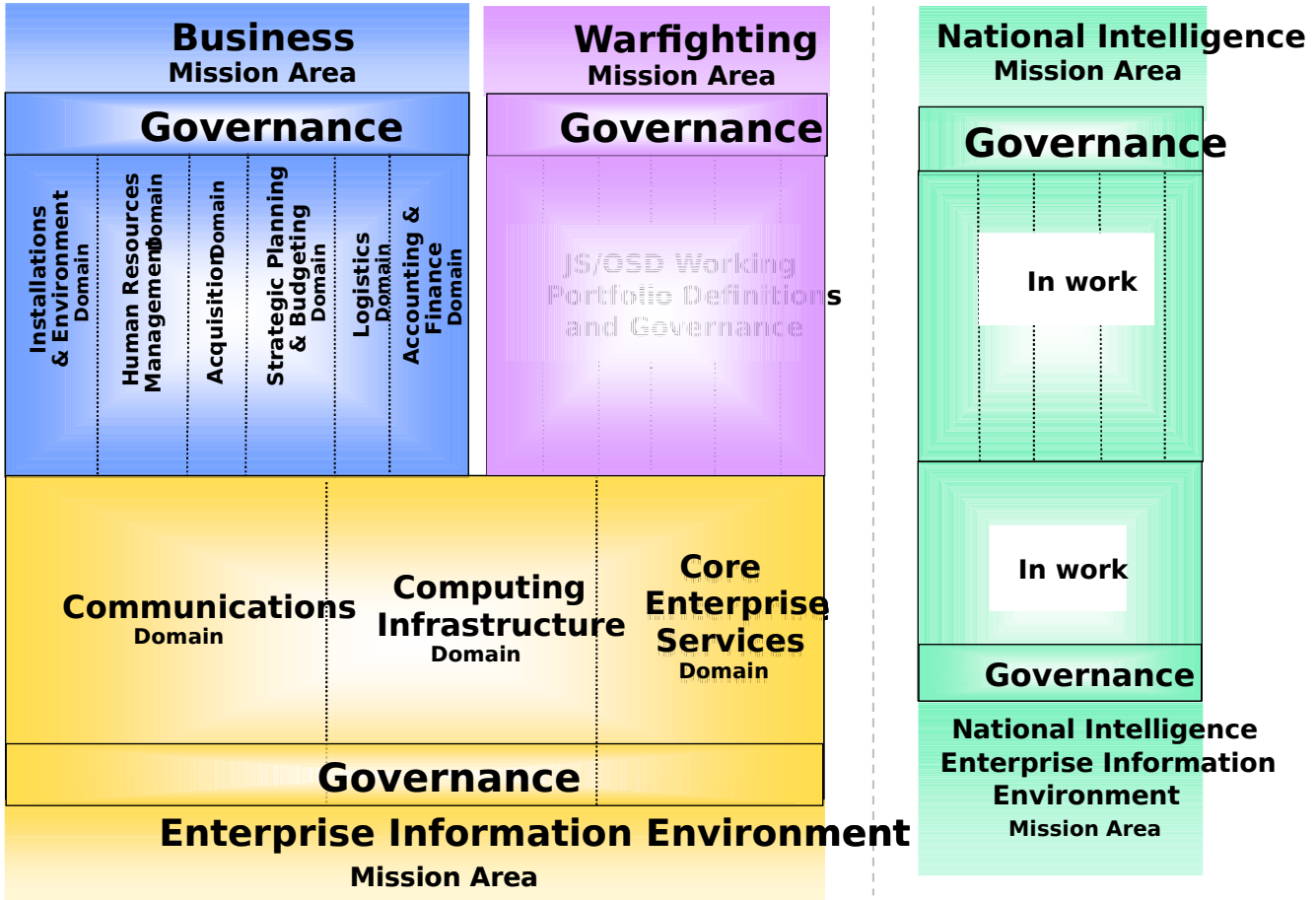
Global Information Grid (GIG)

- The GIG was established March 2000
- The GIG is a globally interconnected, end-to-end set of information capabilities, associated with processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel.
- It includes all owned and leased communications applications, data, security services and other associated services necessary to achieve information superiority.
- Its purpose is to advance department in information management, interoperability and security between and among DoD Components.
- Network Information Infrastructure (NII) and DoD CIO have oversight.

NII's vision is… ***Build the net. Populate it. Protect it.***

Net-Centric Operations Warfare Reference Model (NCOW RM)

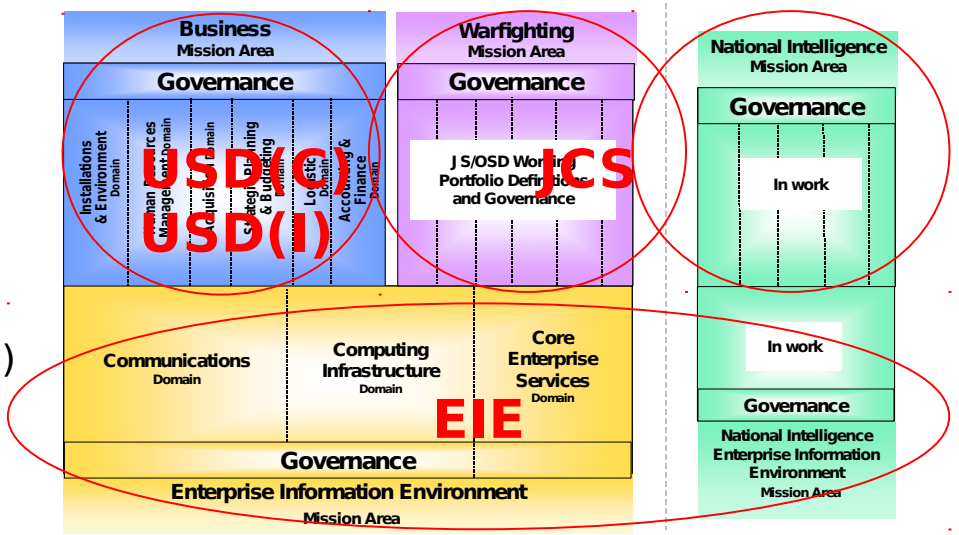
- This represents the target viewpoint for the GIG
- It is a service oriented and inter-networked information infrastructure
- Users request and receive services that enable Business, Warfighting and Enterprise-wide management operations
- It has 3 principle user communities:
  - Business
  - Warfighters
  - Intelligence



DoD Architecture Owners, Users and Providers

Mission Area Owners

- Business – USD(C)/CFO
- Warfighting – Chairman, JCS
- National Intelligence – USD(I) and IC
- Enterprise Information Environment (EIE)
  - ASD NII/CIO (UNCLAS)
  - ASD(NII)/CIO and IC (CLASSIFIED)



Service User

- Warfighting, Business, and National Intelligence Mission Areas provide mission specific capabilities. They use the information capabilities and services provided by the Enterprise Information Environment (EIE) Mission Area.

Service Provider

- The Enterprise Information Environment Mission Area portfolio encompasses the communications, computing and core service systems, equipment, or software that provides a common information capability or service for Enterprise use.

EIE Mission Area responsibilities

- Establish Domains and Portfolio Management Processes
- Maintain an “Objective Mission Area Architecture” and Oversee capability planning that cross multiple Domains
- Coordinate on cross domain issues
  - Identify cross information capabilities and assign to a Domain for governance
  - Assess utility of enterprise-wide capabilities and services
- Lead net-centric transformation
  - Bias investments toward the objective architecture to achieve net-centricity
  - Communicate across the enterprise

NOTE 1: The BEA is the business extension of the Department-wide enterprise architecture, the GIG. Business Domains must adhere to the requirements included in both the GIG and BEA.

NOTE 2: All architectural efforts are required to conform to the requirements of the Federal Enterprise Architecture.

DoD Net Centric data strategy

***Net-Centric*: Exploitation of advancing technology that moves from an application centric to a data-centric paradigm – that is, providing users the ability to access applications and services through Web services – an information environment comprised of interoperable computing and communication components.**

Capability

- Data is to be visible, available, and usable when needed and where needed
- Data is "Tagged" with metadata to enable discovery of data by users
- Data is posted to shared spaces to provide access to all users (except when limited by security, policy, or regulations)
- Data exchanges will no longer be through point-to-point interfaces but "many-to-many" exchanges typical of a network environment

Outcome

- Encourages many-to-many information sharing.
- Data and information will be reused, extended and rapidly exploited
- Better decision making

Net Centric Attributes

- **Internet protocol** –routed across network, not switched via dedicated circuits
- **Secure and available communications**- edge-to-edge encryption
- **Only handle information once** (OHIO)
- **Post in parallel** – information available as soon as it is created
  - Data is tagged and posted before processing
- **Smart pull** – applications support discovery tools; users can pull data directly from the net or use valued added discovery services
  - Data is stored in a public space and advertised (tagged) for discovery
- **Data centric** – Data is separate from applications; applications talk to each other by posting data
  - Data is registered in DoD Metadata Registry
- **Application diversity** – Users can pull multiple applications to access same data
  - Applications are posted to the net and tagged for discovery
- **Assured sharing** – trusted collaborative environment
  - Access assured for authorized users; denied to unauthorized users
- **Quality of service** – data is timely, accurate, complete, easy to use, secure

NII POCs

Architecture Type	POC
GIG Architecture Products NCOW Ref Model GAO Matters	
Combatant Command Architectures	
DOD Architecture Framework CADM (Data model)	
Defense Architecture Repository System (DARS)	
Federal Enterprise Architecture (FEA) OMB Matters	
DOD Joint Technical Architecture (JTA) and IT Standards process	

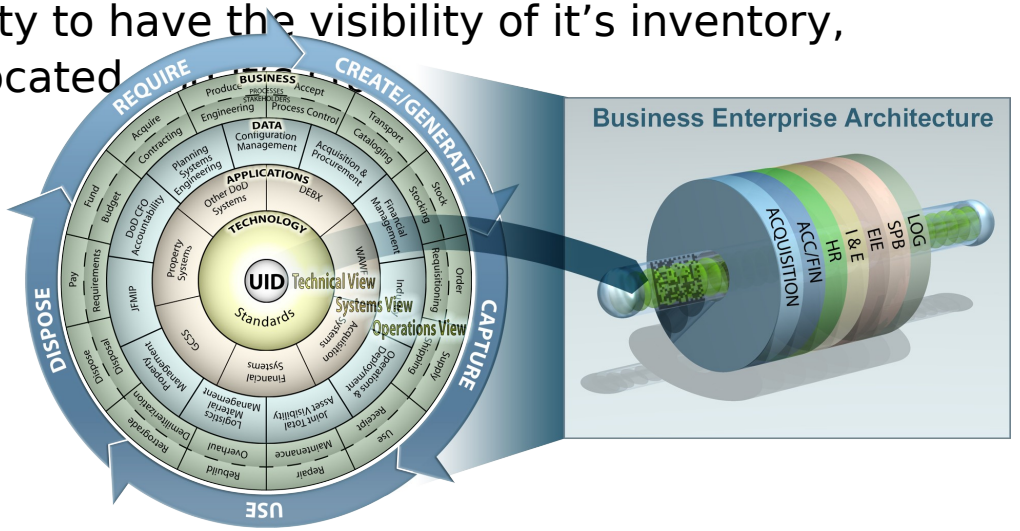
UID and valuation

- **UID is…**
  - **A single data element that is comprised of a set of a concatenated data elements**
  - **Globally unique and unambiguous**
  - **It is used to identify tangible assets - in most cases it must applied to item (label or engraved)**
  - **It requires specific syntax and semantic formats**
  - **It includes a…**
    - Enterprise identifier
    - Serial number
    - Part number (only required if the enterprise serializes within the part number and not the enterprise)
- **DoD has mandated use of UID and DoD has drafted contract language that requires industry to put UIDs on tangible assets and report their values when the assets are delivered**
- **DoD developed required UID format (2 constructs) but will accept certain equivalents**

Just as a Social Security Number is critical to capturing information on people in personnel systems, a universal unique identifier facilitates item tracking in DoD business systems.

UID Benefits and Expectations

- **Property Management** – allows the DoD the ability to establish a single repository for capturing new items of Property, Plant & Equipment as they are introduced into the system. Also, allows the DoD the ability to manage this equipment throughout the world.
- **Financial** - allows DoD the ability to capture the value of each uniquely identified asset for fiscal accountability purposes.
- **Logistical** – allows DoD the ability to have the visibility of it's inventory, available resources, where it is located



✓ ***Enhances Total Asset Visibility***

✓ ***Enhances the BEA***

✓ ***Facilitates Clean audit Opinions***

When is UID required?

Unique identification, or a DoD recognized unique identification equivalent, is required for all items delivered to the Government if:

(1) The acquisition cost is $5,000 or more

(2) It is either a serially managed, mission essential or controlled inventory piece of equipment or reparable item, or a consumable item or material where permanent identification is required

(3) It is a component of a delivered item, if the program manager has determined that unique identification is required, or

(4) A UID or DoD-recognized UID equivalent is available.

memo dated July 29, 2003

How items are to be marked

Construct #1

Enterprise ID		
Serial Number	786950	
Original Part Number	1234	

Construct #2

Enterprise ID		
Serial Number	786950	
Original Part Number	1234	
Original Part Number	1234	

UID Equivalency Criteria

Criteria

- Must contain an enterprise identifier, which is assigned by a registration or controlling authority
- Must uniquely identify an individual item within an enterprise identifier, product or part number
- Must have an existing Data Identifier (DI) or Application Identifier (AI) listed in ANSI MH10.8.2

Compliant alternatives

- **Global Individual Asset Identifier** (GIAI), EAN.UCC (Application Identifier: 8004; Data Identifier: 1B)
- **Global Returnable Asset Identifier** (GRAI), EAN.UCC (Application Identifier: 8003; Data Identifier: 1B or 5B)
- **Vehicle Identification Number** (VIN), ISO 3779 (Data Identifier: I)
- **Electronic Serial Number** (ESN, for cellular telephones only), TIA (Data Identifier: 22S; Application Identifier: 8002)

Enables the use of existing unique identifiers in commercial use

Who marks items with UID?

- **New equipment** – the manufacturer (specified in contract language)
- **Legacy equipment** (Policy evolving) - probably the government at a time that minimizes operational impact (e.g. during maintenance cycles)
- **GFP** - Policy is evolving
  - Marking responsibility will be shared by Industry/PM depending on whether it is legacy or new
  - Objective is to minimize workload
  - Legacy items at contractor sites may use a “virtual” (alias) UID
  - Virtual (alias) UIDs must be recorded in a web enabled GFP Component owned Registry
  - When GFP assets are moved, they must be marked and recorded in the UID registry; the virtual virtual UID should be subsequently deleted from the GFP registry

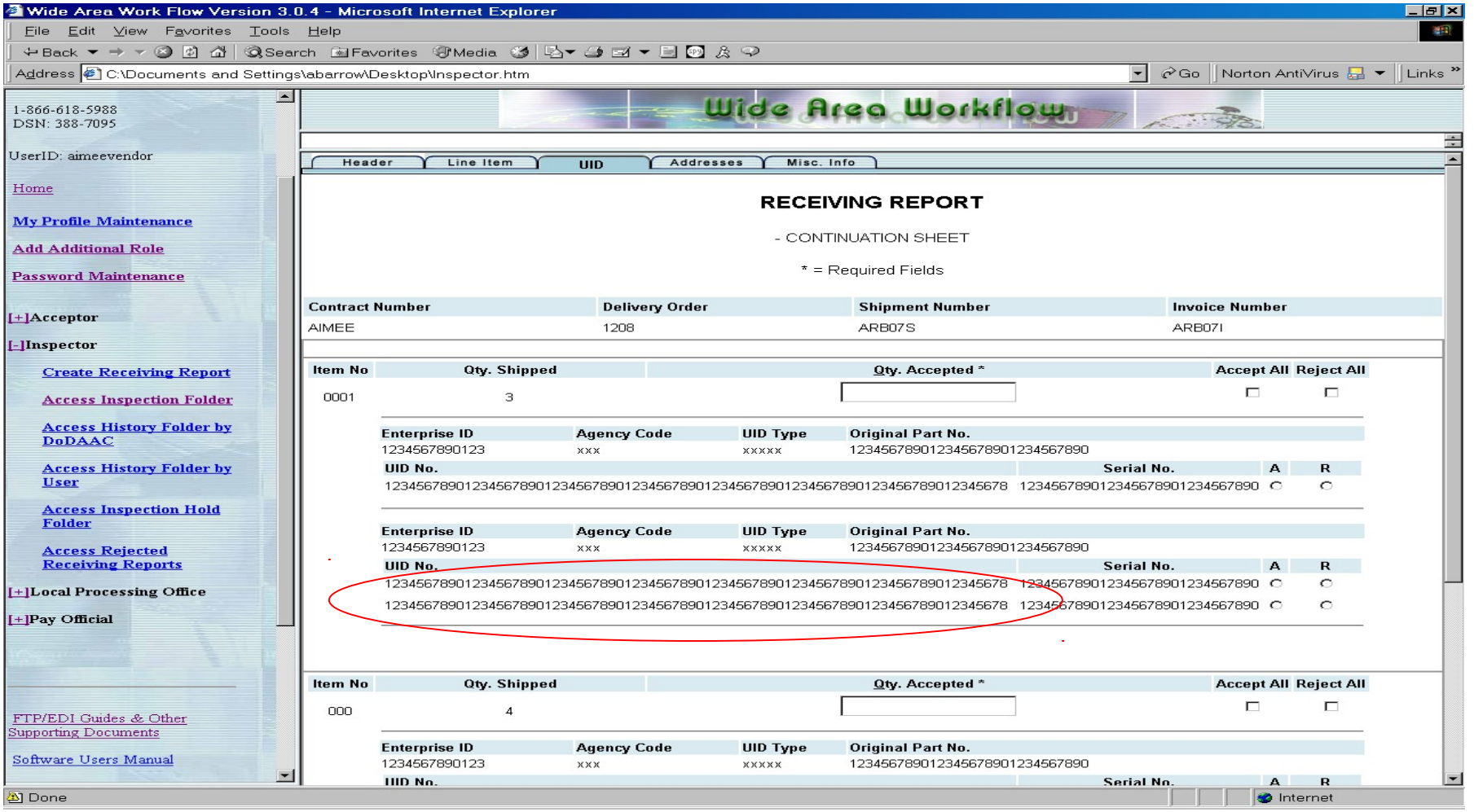
Wide Area Workflow (WAWF)

- **WAWF supports receipt and acceptance processes**
  - Will automate manual DD250 receipt document processes
  - It is mandated DoD-wide in January 05
  - It will incorporate UID requirements
  - It will direct UID information to the “UID Registry”

- **WAWF Deployment**
  - Goal is maximum deployment
  - The Business Initiatives Council (BIC) set a goal of 51% of transactions processed in WAWF by October 1, 2004; Deployment plans were due on December 16, 2003
  - Deployment plans have been received from:
    - Air Force (schedule & implementation)
    - Navy (schedule)
    - DISA (draft schedule & implementation)
    - DCMA
    - Army (implementation plan only)
  - Deployment status will be tracked via metrics

WAWF is the system that will introduce UID into the DoD Business Architect

WAWF Receipt and Acceptance by UID



WAWF UID and Acquisition Data reporting requirements

End Item Data (15)

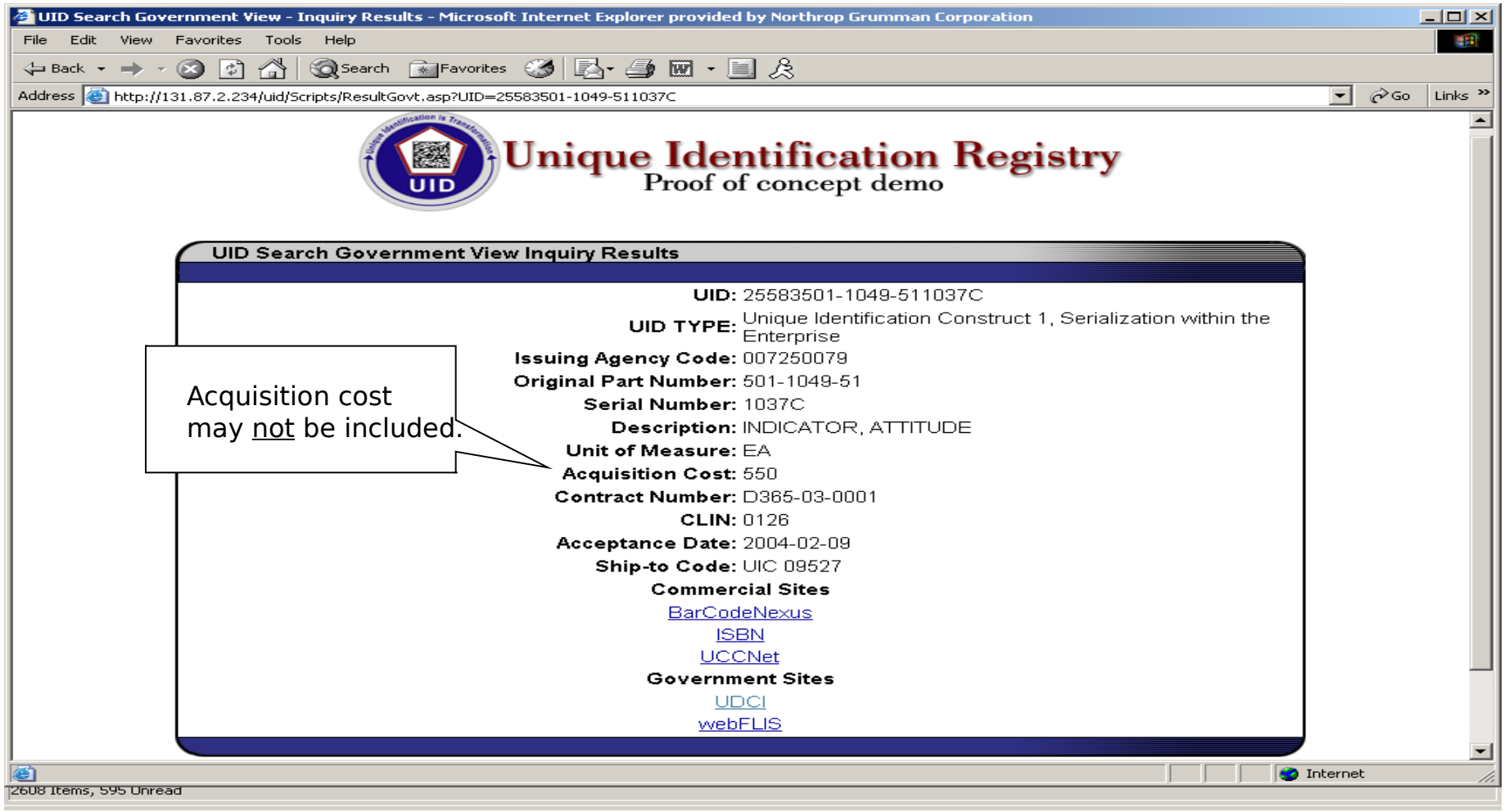
- UID (Concatenated)
- Descriptive Data
  - UID Type
  - Issuing Agency Code
  - Enterprise Identifier
  - Part Number
  - Serial Number
  - Item Description
  - Unit of measure
- Acquisition Data
  - Contractor DUNS
  - Contract Number
  - CLIN/SLIN/ELIN
  - Price
  - Acceptance Location Code (identifies acceptor)
  - Acceptance Date
  - Ship to code

Embedded Items of End Items (10)

- UID (Concatenated)
- Descriptive Data
  - UID Data Elements (5)
  - Item Description
  - Unit of measure
- Parent UID as of delivery date
- GFP flag

- *More data requirements for end-items vs embedded items*
- *Embedded items must include "parent"*
- *GFP will be flagged; this is expected to help with Military Equipment valuations for embedded government furnished materials*

UID Registry



RFID

RFID is a media that carries UID and enables hands-off automated data capture

- Required beginning January 2005 for tagged cases and pallets shipped to DoD receiving points
- Pilots will help determine pace of expansion
- Tags will be EPC-compliant
- Initial Implementation Projects are in progress
- Second DoD RFID Summit for Industry – Apr 04
  - Present EPC requirements to suppliers
- Publish RFID Policy Update – Apr 04
- Develop/Publish proposed DFAR rule for RFID – May 04
- Publish Final RFID Policy – Jul 04
- Publish Final DFAR rule effective Oct 1, 2004 – Sep 04
- Implement RFID – Jan 1, 2005

Impacts on DPAS

GIG

- DPAS will have to become GIG compliant

UID and WAWF

- UID will be added to DPAS
- Current scanners in use may not be able to handle 2D barcodes or UID data requirements (may exceed memory capacity)
- Automating DPAS receiving processes to minimize “fat figuring in” of the UID would be desirable
  - This could be enhanced by creating interfaces with WAWF
  - However, benefit will not be achieved until WAWF is being fully deployed and in use
- Legacy items recorded in DPAS that are $5000 or more will require UIDs (less than 1% of total assets)
  - Policies still evolving how/when to mark legacy and GFP items
  - DPAS will support new policies when they are available
  - UID labels - DPAS could generate UID labels if funding is available and development is permitted

RFID

- DPAS has already tested RFID via pilots but these pilots did not utilize UID